

Sicherheit von Maschinen
Sicherheitsbezogene Teile von Steuerungen
 Teil 2: Validierung
 Deutsche Fassung prEN 954-2 : 1999

DIN
EN 954-2

Einsprüche bis 31. Mai 2000

ICS 13.110

Safety of machinery - Safety-related parts of control systems -
 Part 2: Validation; German version prEN 954-2:1999

Sécurité des machines - Parties des systèmes de commande,
 relatives à la sécurité - Partie 2: Validation;
 Version allemande prEN 954-2:1999

Anwendungswarnvermerk

Dieser Norm-Entwurf wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten an den Normenausschuss Sicherheitstechnische Grundsätze (NASG) im DIN, Burggrafenstr. 6, 10787 Berlin.

Nationales Vorwort

Dieser Norm-Entwurf enthält sicherheitstechnische Festlegungen im Sinne des Gerätesicherheitsgesetzes.

Dieser Norm-Entwurf beinhaltet die Deutsche Fassung des von der gemeinsamen Arbeitsgruppe 6 "Sichere Steuerungen" des Technischen Komitees 114 "Sicherheit von Maschinen und Geräten" des Europäischen Komitees für Normung (CEN) und des Technischen Komitees 44X "Sicherheit von Maschinen und Anlagen; Elektrotechnische Aspekte" des Europäischen Komitees für Elektrotechnische Normung (CENELEC) ausgearbeiteten Norm-Entwurfs prEN 954-2:1999.

Die Deutsche Fassung wurde vom Gemeinschaftsausschuss GA 2 "Steuerungen" des Normenausschusses Sicherheitstechnische Grundsätze (NASG) im DIN erstellt. Es handelt sich hierbei um eine Arbeitsübersetzung. Deshalb enthält dieser Norm-Entwurf, um Missverständnissen aufgrund der Übersetzung zu begegnen, auch die englische Originalfassung, wobei dies keinen wesentlichen Einfluss auf den Preis des Norm-Entwurfs hat.

Die in Abschnitt 2 zitierten Europäischen Normen wurden als DIN-EN-Normen mit gleicher Zählnummer veröffentlicht.

Um Stellungnahmen besser bearbeiten zu können, wird darum gebeten, diese zusätzlich in maschinenlesbarer Form - als Diskette - als Word97-, Word 6.0- oder WordPerfect 5.2-Datei dem NASG zu übermitteln.

Fortsetzung 67 Seiten prEN
 und 60 Seiten Englische Fassung

Normenausschuß Sicherheitstechnische Grundsätze (NASG) im DIN Deutsches Institut für Normung e.V.
 Normenausschuß Maschinenbau (NAM) im DIN
 Deutsche Elektrotechnische Kommission im DIN und VDE (DKE)

– Leerseite –

ICS

Deutsche Fassung

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung

Safety of machinery - Safety-related parts of control systems - Part 2: Validation

Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 2: Validation

Dieser Europäische Norm-Entwurf wird den CEN-Mitgliedern zur Umfrage vorgelegt. Er wurde vom Technischen Komitee CEN/TC 114 erstellt.

Wenn aus diesem Norm-Entwurf eine Europäische Norm wird, sind die CEN-Mitglieder gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Dieser Europäische Norm-Entwurf wurde vom CEN in drei offiziellen Fassungen (Deutsch, Englisch, Französisch) erstellt. Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien, der Tschechischen Republik und dem Vereinigten Königreich.

Warnvermerk : Dieses Schriftstück hat noch nicht den Status einer Europäischen Norm. Es wird zur Prüfung und Stellungnahme vorgelegt. Es kann sich noch ohne Ankündigung ändern und darf nicht als Europäische Norm in Bezug genommen werden.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

Zentralsekretariat: rue de Stassart, 36 B-1050 Brüssel

Inhalt

Seite

Vorwort	3
0 Einleitung	3
1 Anwendungsbereich	4
2 Normative Verweisungen	4
3 Validierungsverfahren	4
3.1 Validierungsleitsätze	4
3.2 Validierungsplan	7
3.3 Dokumente für die Validierung	7
3.4 Validierungsaufzeichnung	8
4 Validierung durch Analyse	8
4.1 Allgemeines	8
4.2 Analysentechniken	9
5 Validierung durch Prüfen	9
5.1 Allgemeines	9
5.2 Umgebungsbedingungen	10
5.3 Meßwertgenauigkeit	10
5.4 Höherwertige Festlegungen	10
5.5 Anzahl der Prüflinge	11
6 Fehlerlisten	11
6.1 Allgemeine Fehlerlisten	11
6.2 Spezielle Fehlerlisten	11
7 Validierung der Sicherheitsfunktionen	12
8 Validierung der Kateorien	12
8.1 Allgemeines	12
8.2 Prüfung der Kategorien	12
8.3 Validierung der Festlegungen für Kategorie	13
8.4 Validierung der Kombination von sicherheitsbezogenen Teilen.....	14
9 Validierung der Umgebungsanforderungen	14
10 Validierung der Instandhaltungsanforderungen	14
Anhang A (informativ) Möglichkeiten zur Validierung mechnischer Systeme	15
Anhang B (informativ) Möglichkeiten zur Validierung pneumatischer Systeme	21
Anhang C (informativ) Möglichkeiten zur Validierung hydraulischer Systeme	36
Anhang D (informativ) Möglichkeiten zur Validierung elektrischer Systeme	49
Anhang ZA (informativ) Abschnitte in dieser Europäischen Norm, die grundlegende oder andere Vorgaben von EU-Richtlinien betreffen	65
Literaturhinweise	66

Vorwort

Diese Europäische Norm wurde vom Technischen Komitee CEN/TC 114 "Sicherheit von Maschinen" erarbeitet, dessen Sekretariat vom DIN gehalten wird.

Diese Europäische Norm wurde im Rahmen eines Mandates, das dem CEN von der Europäischen Kommission und der Europäischen Freihandelszone erteilt wurde, erarbeitet wurde, erarbeitet und unterstützt grundlegende Anforderungen der EU-Richtlinie(n).

Diese Norm hat den Status einer Anwendungsnorm (Typ B 1).

Entsprechend der CEN/CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu

0 Einleitung

Diese Europäische Norm legt das Validierungsverfahren, einschließlich der beiden Verfahren Analyse und Prüfung, für die Sicherheitsfunktionen und Kategorien von sicherheitsbezogenen Steuerungen fest. Beschreibungen der Sicherheitsfunktionen und die Anforderungen für die Kategorien sind in EN 954-1 gegeben, die sich mit den allgemeinen Leitsätzen für die Gestaltung befaßt.

Einige Anforderungen für die Validierung sind allgemeiner und einige spezifischer Art entsprechend der angewendeten Technologie. prEN 954-2 legt auch die Bedingungen fest unter welchen die Validierung beim Testen der sicherheitsbezogenen Teile von Steuerungssystemen durchgeführt werden sollte.

EN 954-1 legt die Sicherheitsanforderungen fest und gibt Anleitung für die Leitsätze bei der Gestaltung (siehe EN 292-1: 1991, 3.11) der sicherheitsbezogenen Teile von Steuerungen. Sie legt für diese Teile die Kategorie fest und beschreibt die speziellen Eigenschaften ihrer Sicherheitsfunktion unabhängig von der verwendeten Energieart.

Das Erreichen der Anforderungen kann durch alle möglichen Kombinationen der Analyse (siehe Abschnitt 4) und der Prüfung (siehe Abschnitt 5) validiert werden. Mit der Analyse sollte so früh wie möglich und gleichzeitig mit den Gestaltungsprozeß begonnen werden, damit Probleme früh ausgeräumt werden können und sie in dieser Phase noch relativ leicht zu korrigieren sind, wie z.B. im Verlauf der Schritte 3 und 4 im EN 954-1: 1996, 4.3 beschrieben. Für einige Analysen kann es erforderlich sein, sie bis zur einer zufriedenstellenden Gestaltung zu verschieben.

Die Anhänge A bis D sind informativer Art und strukturiert wie in Tabelle 1 angegeben.

Tabelle 1: Aufbau der Abschnitte der Anhänge A bis D

Anhang	Technologie	Liste der grundlegenden Sicherheitsprinzipien	Liste der bewährten Sicherheitsprinzipien	Liste der bewährten Bauteile	Fehlerlisten und Fehlerabschlüsse
		Abschnitt			
A	Mechanik	A..1	A. 2	A. 3	A. 4
B	Pneumatik	B. 1	B. 2	B. 3 (leer)	B. 4
C	Hydraulik	C. 1	C. 2	C. 3 (leer)	C. 4
D	Elektrik	D. 1	D. 2	D. 3	D. 4

1 Anwendungsbereich

Diese Europäische Norm legt die Vorgehensweisen und Bedingungen fest, die bei der Validierung durch Analyse und Prüfung zu befolgen sind, für

- die vorgesehenen Sicherheitsfunktionen und
- die ausgeführten Kategorien

Der sicherheitsbezogenen Teile von Steuerungen, bei Anwendung der durch den Konstrukteur vorgesehenen sinnvollen Gestaltung und in Übereinstimmung mit EN 954-1.

Im Gegensatz zum Anwendungsbereich der EN 954-1 : 1996 enthält diese Norm keine speziellen Anforderungen für programmierbare elektronische Systeme, wenn sie Sicherheitsfunktionen bei Maschinenanwendungen erfüllen. Folglich gibt dieser Teil 2 keine vollständigen Validierungsanforderungen für programmierbare elektronische Systeme. In Steuerungen, die bei der Durchführung von Sicherheitsfunktionen programmierbare elektronische Systeme einschließen, ist die Anwendung von Kategorien nicht ausreichend, wenn:

- 1) die Sicherheitsfunktion der Steuerungen allein vom programmierbaren elektronischen System abhängt, oder
- 2) die Struktur der Steuerung komplex ist, oder
- 3) der Beitrag der Risikominderung an der Maschine durch die Steuerung hoch ist.

In diesen Fällen sollten zusätzliche Faktoren (z. B. systematische Fehler) ebenfalls berücksichtigt werden.

ANMERKUNG: JWG 6 schlägt vor, die Ausführungen hierzu bei der Erarbeitung der Änderung zu Teil 1 der EN 954-1 einzubringen. Eine Anwendungsnorm für Maschinen, der die IEC 61508 zugrunde liegt, wird zur Zeit von der IEC/TC 44/WG 7 erarbeitet.

2 Normative Verweisungen

Diese Europäische Norm enthält durch datierte oder undatierte Verweisungen Festlegungen aus anderen Publikationen. Diese normativen Verweisungen sind an den jeweiligen Stellen im Text zitiert und die Publikationen sind nachstehend aufgeführt. Bei datierten Verweisungen gehören spätere Änderungen oder Überarbeitungen dieser Publikation nur zu dieser Europäischen Norm, falls sie durch Änderung oder Überarbeitung eingearbeitet sind. Bei undatierten Verweisungen gilt die letzte Ausgabe der in Bezug genommenen Publikation.

- | | |
|-----------------|---|
| EN 292-1 : 1991 | Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze – Teil 1: Grundsätzliche Terminologie, Methodologie |
| EN 954-1 : 1996 | Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze |

3 Validierungsverfahren

3.1 Validierungsleitsätze

Der Zweck der Validierung ist, die Festlegungen und das Niveau der Konformität der sicherheitsbezogenen Teile der Steuerung innerhalb der Gesamtfestlegungen für die Sicherheitsanforderungen an der Maschine zu bestätigen.

Die Validierung muß aufzeigen, daß jedes sicherheitsbezogene Teil die Anforderungen von EN 954-1 erfüllt, insbesondere bei

- den festgelegten Sicherheitseigenschaften für diesen Teil, wie in der sinnvollen Gestaltung realisiert, und
- bei den Anforderungen für die festgelegte Kategorie (siehe EN 954-1 : 1996, Abschnitt 6).

Die Validierung besteht aus der Durchführung der Analyse (siehe Abschnitt 4) und, soweit notwendig, aus der Durchführung von Prüfungen (siehe Abschnitt 5) in Übereinstimmung mit dem Validierungsplan. Bild 1 gibt einen Überblick über das Validierungsverfahren.

Für umfangreiche und/oder komplexe Systeme können aufgrund der Größe, Komplexität oder integrierten Art (mit der Maschine) der Steuerung spezielle Zusammenstellungen gemacht werden für die:

- Validierung der sicherheitsbezogenen Teile der Steuerung gesondert vor dem Einbau;
- Simulation der angemessenen Eingangs- und Ausgangssignale;
- Validierung der Auswirkungen bei Integration der sicherheitsbezogenen Teile in den Rest der Steuerung und die Maschine als Ganzes.

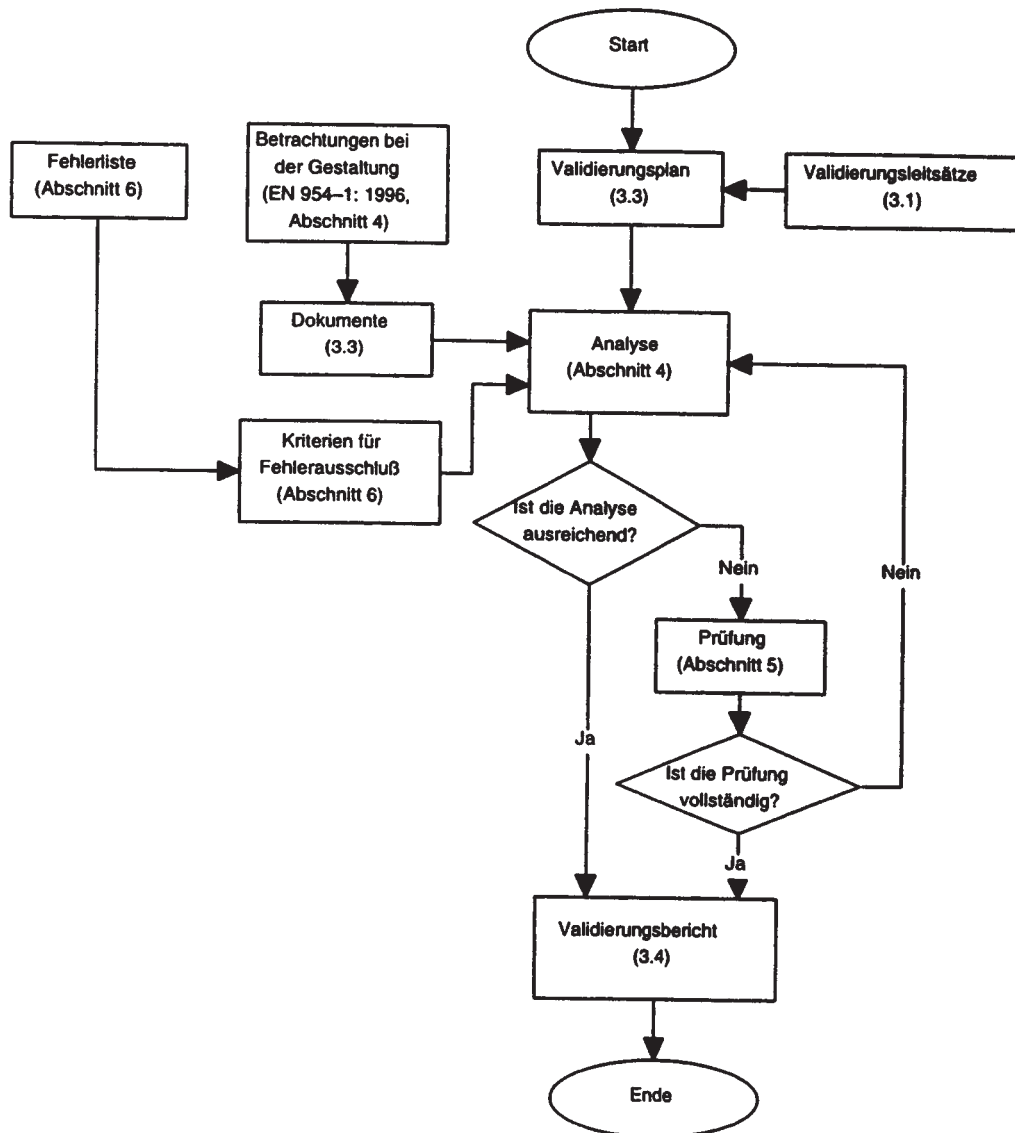


Bild 1: Übersicht über das Validierungsverfahren

3.2 Validierungsplan

Der Validierungsplan muß die Anforderungen für die Durchführung des Validierungsverfahrens für die festgelegten Sicherheitsfunktionen und ihrer Kategorien identifizieren und beschreiben.

Der Validierungsplan muß auch die Mittel identifizieren, die zu benutzen sind um die festgelegten Sicherheitsfunktionen und Kategorien zu validieren. Wo es angemessen ist, muß er aufzeichnen:

- a) die Identität der Dokumente für die Festlegungen;
- b) die Betriebs- und Umgebungsbedingungen;
- c) die grundlegenden Sicherheitsprinzipien (siehe A.1, B.1, C.1 und D.1);
- d) die bewährten Sicherheitsprinzipien (siehe A.2, B.2, C.2 und D.2);
- e) die bewährten Bauteile (siehe A.3 und D.3);
- f) die Fehler, die aus den Fehlerlisten in A.4, B.4, C.4 und D.4 zu berücksichtigen sind;
- g) alle Analysen und Prüfungen, die angewandt wurden.

3.3 Dokumente für die Validierung

Die Dokumente, die für die Validierung erforderlich sind, unterscheiden sich hinsichtlich der angewendeten Technologie, der Kategorie(n), die aufzuzeigen sind, und hinsichtlich der sinnvollen Gestaltung des Systems. Ausreichende Dokumente entsprechend der untenstehenden Auflistung müssen zum Validierungsverfahren einbezogen werden, um die erreichten Kategorie(n) und die Sicherheitsfunktion(en) der sicherheitsbezogenen Teile aufzuzeigen.

- a) Festlegung(en) über die angenommene Leistungsfähigkeit der Konstruktion, einschließlich der Sicherheitsfunktionen und Kategorien;
- b) Zeichnungen und Festlegungen, z. B. für mechanische, hydraulische und pneumatische Teile, gedruckte Steuerkreispläne, Montagepläne, interne Verdrahtung, Gehäuse, Materialien, Aufstellung;
- c) Blockdiagramm(e) mit Funktionsbeschreibung der Blöcke;
- d) Steuerkreisdiagramm(e) einschließlich ihrer Verknüpfungen/Verbindungen;
- e) Funktionsbeschreibung der Steuerkreisdiagramme;
- f) Zeitfolgediagramm(e) für schaltende Bauteile, für Signale, die für die Sicherheit zuständig sind;
- g) Bauteilliste mit Stückbezeichnung, Nennwerten, Toleranzen, relevanten weiteren Daten, die für die Sicherheit relevant sind;
- h) Analyse aller relevanten Fehler, die in A.4, B.4, C.4 und D.4 aufgelistet sind, einschließlich der Begründung aller ausgeschlossenen Fehler;
- i) Analyse des Einflusses der im Verfahren verwendeten Materialien;
- k) spezielle Information für die Kategorie nach Tabelle 2;
- l) wo angebracht, muß die Software-Dokumentation beinhalten:
 - 1. eine Festlegung, die klar und eindeutig ist, und die das Erreichen der geforderten sicherheitstechnischen Leistungsfähigkeit der Software bestätigt, und
 - 2. den Beweis, daß die Software so gestaltet ist, daß sie die geforderte sicherheitstechnische Leistungsfähigkeit erreicht, und
 - 3. Einzelheiten über Prüfungen (insbesondere Prüfberichte), die durchgeführt wurden, um zu bestätigen, daß die geforderte sicherheitstechnische Leistungsfähigkeit erreicht wurde.

Tabelle 2: Anforderungen an die Dokumentation für Kategorien

Anforderungen an die Dokumentation	Kategorie, für die eine Dokumentation erforderlich ist				
	B	1	2	3	4
Grundlegende Sicherheitsprinzipien	x	x	x	x	x
Zu erwartende Betriebsbeanspruchungen	x	x	x	x	x
Einfluß des zu verarbeitenden Materials	x	x	x	x	x
Leistungsfähigkeit während anderer relevanter externer Einflüsse	x	x	x	x	x
Bewährte Bauteile	-	x	-	-	-
Bewährte Sicherheitsprinzipien	-	x	x	x	x
Das Prüfverfahren für die Sicherheitsfunktion(en)	-	-	x	-	-
Festgelegte Prüfintervalle	-	-	x	-	-
Bei der Gestaltung berücksichtigte vorhersehbare Einzelfehler und das angewendete Erkennungsverfahren	-	-	-	x	x
Alle identifizierte Fehler gemeinsamer Ursache und wie sie verhindert werden	-	-	-	x	x
Alle vorhersehbaren ausgeschlossenen Einzelfehler	-	-	-	x	x
Wie die Sicherheitsfunktion bei jedem Fehler aufrechterhalten bleibt	-	-	-	x	x
Fehler, die zu erkennen sind	-	-	x	x	x
Verschiedene Fehleranhäufungen, die bei der Gestaltung zu berücksichtigen sind	-	-	-	-	x
Wie die Sicherheitsfunktion bei allen Fehlerkombinationen aufrechterhalten bleibt	-	-	-	-	x

3.4 Validierungsaufzeichnung

Die Validierung durch Analyse und Prüfung muß aufgezeichnet werden. Die Aufzeichnung muß das Validierungsverfahren aller sicherheitstechnischen Anforderungen ersichtlich machen. Es können Querverweise zu anderen Dokumenten gemacht werden, vorausgesetzt sie sind richtig identifiziert.

Für jedes System oder Bauteil, das einen Teil des Validierungsverfahrens nicht bestanden hat, muß die Aufzeichnung zeigen, inwieweit Übereinstimmung mit dieser Norm besteht.

4 Validierung durch Analyse

4.1 Allgemeines

Die Validierung von sicherheitsbezogenen Teilen von Steuerungen muß durch eine Analyse erfolgen. In die Analyse gehen ein:

- die identifizierten Gefährdungen, die sich bei der Gefährdungsanalyse an der Maschine ergeben (siehe EN 954-1 : 1996, Bild 1);
- die Zuverlässigkeit (siehe EN 954-1 : 1996, 4.2);

- die Systemstruktur (siehe EN 954-1 : 1996, 4.2);
- die nicht quantifizierbaren qualitativen Aspekte, die Auswirkung auf das Systemverhalten haben (siehe EN 954-1 : 1996, 4.2);
- deterministische Argumente.

Bei der Validierung der Sicherheitsfunktionen durch Analyse ist weit mehr als bei der Prüfung der Festlegung von deterministischen Argumenten erforderlich. Deterministische Argumente unterscheiden sich von anderen Beweisführungen dadurch, daß sie zeigen, daß die geforderten Eigenschaften des Systems einem Systemmodell logisch folgen. Solche Argumente können auf der Grundlage einfacher, gut verständlicher Begriffe entwickelt werden, wie z. B. die Genauigkeit einer mechanischen Verriegelung.

ANMERKUNG: Ein deterministisches Argument für die Korrektheit eines sicherheitsbezogenen Relaisystems kann auf einer Fallanalyse basieren, die einen Schaltplan benutzt, unterstützt durch die Beweisführung, daß das Produktionssystem mit dem Schaltplan übereinstimmt.

4.2 Analysetechniken

Die auszuwählende Analysetechnik hängt von der Zielrichtung der Analyse ab. Es bestehen zwei grundsätzliche Arten von Techniken:

- a) „Top-down“ (deduktive) Techniken sind zur Bestimmung der Ursachen geeignet, die zu den festgestellten Ausgangsereignissen führen können und zur Abschätzung der Wahrscheinlichkeit von Ausgangsereignissen abhängig von der Wahrscheinlichkeit der Ursachen. Sie können auch angewendet werden bei der Untersuchung der Folgen von erkannten Mehrfachfehlern. Beispiele für „top-down“ Techniken sind die Fehlerbaumanalyse (FTA – siehe IEC 61025) und die Ereignisbaumanalyse (ETA).
- b) „Bottom-up“ (induktive) Techniken sind für die Untersuchung der Folgen von festgestellten Einzelfehlern geeignet. Beispiele für „bottom-up“ Techniken sind die Fehlerarten und Auswirkungsanalyse (FMEA – siehe IEC 60812) und die Fehlerarten, Auswirkungs- und kritischen Zustandsanalysen (FMECA).

EN 1050 : 1996, Anhang B enthält mehr Informationen zu Analysemethoden.

5 Validierung durch Prüfen

5.1 Allgemeines

Wenn die Validierung durch Analyse nicht ausreichend das Erreichen der festgelegten Sicherheitsfunktionen und Kategorien zeigt, müssen Prüfungen durchgeführt werden, um die Validierung zu vervollständigen.

Die Validierung durch Prüfungen muß systematisch geplant und bezogen werden.

Das sind im einzelnen:

- a) Ein Prüfplan muß vor Beginn der Prüfungen ausgearbeitet werden, der folgendes beinhalten muß:
 - 1) die Prüfspezifikation;
 - 2) die zu erwartenden Ergebnisse der Prüfungen;
 - 3) die Reihenfolge der Testungen.
- b) Prüfaufzeichnungen müssen erstellt werden, die folgendes beinhalten:
 - 1) den Namen des Prüfers;
 - 2) die Umgebungsbedingungen (siehe 5.2);
 - 3) die Vorgehensweisen bei der Prüfung und die benutzten Ausrüstungen;
 - 4) die Ergebnisse der Prüfungen.

- c) die Prüfaufzeichnungen müssen mit dem Prüfplan verglichen werden, um Gewißheit zu erhalten, daß die festgelegten Funktions- und Leistungsziele die festgelegten Werte erreicht haben.

Diese Prüfungen können manuell oder automatisch, z. B. durch Rechner, durchgeführt werden.

Wo angebracht, muß die Validierung von Sicherheitsfunktionen durch Prüfung durchgeführt werden, bei der Signale in verschiedenen Kombinationen in die sicherheitsbezogenen Teile der Steuerung eingegeben werden. Die korrespondierenden Ausgänge müssen mit den entsprechend festgelegten Ausgangssignalen verglichen werden.

Es wird empfohlen, daß die Anwendung dieser Eingangssignale systematisch der Steuerung und der Maschine anzupassen ist. Ein Beispiel für diese Logik ist: Energie einschalten, starten, Arbeitsablauf, Bewegungsumkehr, Wiederanlauf. Wo notwendig, muß eine erweiterte Anzahl Eingangsdaten eingegeben werden, um anormale oder ungewöhnliche Situationen zu berücksichtigen, und um zu sehen, wie die sicherheitsbezogenen Teile der Steuerung reagieren. Solche Kombinationen von Eingangsdaten müssen vorhersehbare inkorrekte Abläufe berücksichtigen.

5.2 Umgebungsbedingungen

Soweit nicht anderweitig festgelegt, müssen die Validierungsprüfungen mit einer Steuerung durchgeführt werden, die bei normalen und Nennwertbedingungen arbeitet, wie sie in den Begleitdokumenten oder auf dem Kennzeichenschild angegeben sind. Der Prüfling muß auch so nahe wie möglich an seiner endgültigen Betriebsweise arbeiten, d. h. mit allen beigelegten peripheren Einrichtungen und Abdeckungen.

Die relevanten Umgebungsbedingungen unter denen die Validierungsprüfungen durchgeführt wurden, müssen aufgezeichnet werden. Eine Checkliste für Umgebungsbedingungen, die Einfluß auf die Validierungsprüfung haben können, ist im Abschnitt 9 gegeben.

Die Prüfungen müssen unter stabilen Bedingungen durchgeführt werden. Der Umfang, bei dem die Bedingungen als stabil angesehen werden können und bei dem Prüfungen gültig sind, müssen zwischen dem Konstrukteur und dem Personal, das die Prüfungen durchführt, abgestimmt und aufgezeichnet werden.

Transiente Veränderungen am Ausgang der sicherheitsbezogenen Teile von Steuerungen sind tragbar, falls die festgelegte Veränderung über die Zeit von einem Zustand in einen anderen Zustand am Ausgang größer ist, als die Zeitdauer der transienten Veränderung.

5.3 Meßwertgenauigkeit

Soweit nicht anderweitig festgelegt, muß die Genauigkeit der Messung bei der Validierung durch Prüfung für Temperaturmessungen innerhalb ± 5 K und die Genauigkeit der Messung bei der Validierung durch Prüfung für:

- a) Zeitmessungen,
- b) Druckmessungen,
- c) Kraftmessungen,
- d) Elektrische Messungen (wo technisch möglich und/oder angemessen),
- e) Relative Feuchtigkeitsmessungen,
- f) Abstandsmessungen,

muß bei ± 5 % liegen.

5.4 Höherwertige Festlegungen

Wenn entsprechend den Angaben in den Begleitdokumenten die Steuerung höherwertige Festlegungen als nach den Anforderungen dieser Norm erfüllt, müssen die höherwertigen Festlegungen zugrundegelegt werden.

ANMERKUNG: Derartig höherwertige Festlegungen können zugrundegelegt werden, wenn die Steuerung besonders ungünstigen Betriebsbedingungen standhalten muß, z. B. raue Handhabung, Feuchtigkeitseinwirkungen, Hydrolyse, Veränderungen bei der Umgebungstemperatur, Auswirkungen von chemischen Agenzien, Korrosion, hohe Intensität elektromagnetischer Felder, zum Beispiel in der Nähe von Sendern.

5.5 Anzahl der Prüflinge

Soweit nicht anderweitig festgelegt, müssen die Prüfungen an einem einzelnen Muster durchgeführt werden, das allen relevanten Prüfungen standhalten sollte.

Gegenstände, die sich in der Prüfung befinden, dürfen während des Prüfablaufes nicht verändert werden.

Einige Prüfungen können ständig die Leistungsfähigkeit einiger Bauteile verändern. Wo die ständige Veränderung in den Bauteilen der Grund dafür ist, daß die sicherheitsbezogenen Teile von Steuerungen außerhalb der Gestaltungsfestlegungen liegen, kann es notwendig sein, weitere Muster für nachfolgende Prüfungen zu benutzen.

Wo eine bestimmte Prüfung zerstörend wirkt und gleichwertige Ergebnisse durch Prüfung erhalten werden können, bei der ein Teil der Ausrüstung abgetrennt wird, kann ein Muster dieses Teiles anstelle des gesamten Ausrüstungsmusters benutzt werden, um an das Ergebnis für diese Prüfung zu gelangen.

6 Fehlerlisten

6.1 Allgemeine Fehlerlisten

Das Validierungsverfahren schließt die Überlegung des Verhaltens von sicherheitsbezogenen Teilen der Steuerungen im Fehlerfall ein. Zu berücksichtigende Fehler sind in den allgemeinen Fehlerlisten in A.4, B.4, C.4 und D.4 zu finden, die sich auf Erfahrungen abstützen. Die allgemeinen Fehlerlisten enthalten:

- die einzubeziehenden Bauteile/Elemente, z. B. Leiter, Kabel (siehe D.4.1);
- die zu berücksichtigenden Fehler, z. B. Kurzschlüsse zwischen Leitern;
- die erlaubten Fehlerausschlüsse;
- eine Spalte für Bemerkungen, die die Begründungen für Fehlerausschlüsse enthält.

Nur permanente Fehler sind berücksichtigt.

6.2 Spezielle Fehlerlisten

Eine spezielle Fehlerliste muß als Bezugsdokument für das Validierungsverfahren für die sicherheitsbezogenen Teile erstellt werden. Dieser Liste müssen die entsprechenden allgemeinen Listen in den Anhängen zugrunde liegen.

Diese Liste muß bestätigen:

- die aus den allgemeinen Listen einbezogenen Fehler;
- alle anderen relevanten einbezogenen Fehler, die nicht in der allgemeinen Liste aufgeführt sind (z. B. transiente Fehler, Fehler mit gemeinsamer Ursache);
- die aus der allgemeinen Liste entnommenen Fehler, die ausgeschlossen werden dürfen und schließlich die Kriterien befriedigen können, die in den allgemeinen Listen enthalten sind (siehe EN 954-1:1996, 7.2),
- alle anderen relevanten Fehler aus der allgemeinen Liste, für die die allgemeine Liste jedoch einen Ausschluß nicht zuläßt, zusammen mit einer Begründung und sinnvollen Erklärung für ihren Ausschluß (siehe EN 954-1:1996, 7.2).

Jede Abweichung von den allgemeinen Listen muß begründet sein.

7 Validierung der Sicherheitsfunktionen

Ein wichtiger Schritt für eine vollständige Übereinstimmung mit ihren festgelegten Eigenschaften ist die Validierung der Sicherheitsfunktionen (von sicherheitsbezogenen Teilen der Steuerung). Beim Formulieren der Festlegungen und während der Entwicklung der Maschine ist es wichtig, Irrtümer und besonders Unterlassungen abzufragen.

Das Ziel der Validierung von Sicherheitsfunktionen ist sicherzustellen, daß sicherheitsbezogene Ausgangssignale abhängig von den Eingangssignalen entsprechend den Festlegungen korrekt und logisch sind. Die Validierung sollte alle normalen und vorhersehbaren abnormalen Bedingungen durch statische und dynamische Simulation abdecken.

Die festgelegten Sicherheitsfunktionen (nach EN 954-1:1996, Abschnitt 5) müssen in allen Betriebsarten der Maschine validiert werden. Das heißt:

- die Validierung muß durchgeführt werden, um die korrekte Funktion bei verschiedenen Konfigurationen zu demonstrieren und um ausreichend sicherzustellen, daß alle sicherheitsbezogenen Ausgangssignale über ihren gesamten Bereich verwirklicht sind. Prüfungen (z. B. Überlastprüfungen, Drehzahlüberschreitungsprüfungen) können notwendig sein, um die festgelegten Sicherheitsfunktionen zu validieren.
- die Validierung muß durchgeführt werden, um die korrekte Funktion durch Reaktion auf vorhersehbare abnormale Signale von irgendeiner Eingangsquelle unter Einbeziehung der Energieunterbrechung und –wiederkehr zu demonstrieren.

8 Validierung der Kategorien

8.1 Allgemeines

Die Validierung der Kategorien muß zeigen, daß ihre Anforderungen erfüllt sind. Grundsätzlich sind die folgenden Verfahren anwendbar:

- eine Analyse der Steuerkreisdiagramme (siehe Abschnitt 4);
- Prüfungen bei den tatsächlich vorhandenen Steuerkreisen und Fehlersimulation an den tatsächlich vorhandenen Bauteilen, besonders in zweifelhaften Bereichen, hinsichtlich der bei der Analyse festgestellten Leistungsfähigkeit (siehe Abschnitt 5);
- eine Simulation des Verhaltens der Steuerung, z. B. mit Mitteln von Hardware und/oder Softwaremodellen.

Wenn in einigen Anwendungsfällen die sicherheitsbezogenen Teile der Steuerung in komplexer Weise verbunden sind, ist es üblicherweise notwendig, die verbundenen sicherheitsbezogenen Teile in verschiedene Funktionsgruppen zu trennen und diese Gruppen und ihre Verknüpfungen Fehlersimulationsprüfungen zu unterziehen (siehe auch Abschnitt 1).

8.2 Prüfung der Kategorien

Bei der Durchführung der Validierung durch Prüfung, können die Prüfungen sofern angemessen, beinhalten:

- Fehlereingabeproofungen an einem Produktionsmuster,
- Fehlereingabeproofungen an einem Hardwaremodell,
- Softwaresimulation von Fehlern,
- Subsystemfehler, z. B. Energieversorgung.

Der genaue Zeitpunkt bei dem ein Fehler in ein System eingegeben wird, kann kritisch sein. Der „worst case effect“ bei einer Fehlereingabe sollte anhand einer Analyse bestimmt werden und der Fehler sollte entsprechend dieser Analyse bei der angemessenen kritischen Zeit eingegeben werden.

8.3 Validierung der Festlegungen für Kategorie

8.3.1 Kategorie B

Die sicherheitsbezogenen Teile von Steuerungen der Kategorie B müssen in Übereinstimmung mit den grundlegenden Sicherheitsprinzipien validiert werden (siehe A.1, B.1, C.1 und D.1) durch Aufzeigen, daß die Spezifikation, die Gestaltung, Konstruktion und Wahl der Bauteile mit EN 954-1:1996, 6.2.1 übereinstimmen. Dies muß durch Prüfen der sicherheitsbezogenen Teile der Steuerung in Übereinstimmung mit ihren Spezifikationen erreicht werden wie sie in den Dokumenten für die Validierung vorgesehen sind (siehe 3.3). Für die Validierung der Umgebungsbedingungen siehe 5.2.

8.3.2 Kategorie 1

Die sicherheitsbezogenen Teile von Steuerungen der Kategorie 1 müssen validiert werden, um aufzuzeigen, daß:

- a) sie die Anforderungen der Kategorie B erfüllen,
- b) die Bauteile bewährt sind (siehe A.3 und D.3) unter mindestens einer der folgenden Bedingungen:
 - 1) sie sind in zahlreichen Fällen mit erfolgreichen Ergebnissen bei ähnlichen Anwendungen benutzt worden;
 - 2) sie sind hergestellt worden nach Prinzipien, die ihre Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen aufzeigen;
- c) die bewährten Sicherheitsprinzipien (siehe A.2, B.2, C.2 und D.2) korrekt einbezogen wurden. Wo neu entwickelte Prinzipien angewandt wurden, muß folgendes validiert werden:
 - 1) wie die zu erwartenden Ausfallarten vermieden wurden;
 - 2) wie Fehler vermieden und ihre Wahrscheinlichkeit reduziert wurde.

Zutreffende Bauteilnormen können benutzt werden, um die Übereinstimmung mit diesem Unterabschnitt aufzuzeigen (siehe A.2 bis D.3).

8.3.3 Kategorie 2

Sicherheitsbezogene Teile von Steuerungen der Kategorie 2 müssen validiert werden, um aufzuzeigen, daß:

- a) sie die Anforderungen der Kategorie B erfüllen,
- b) die angewandten bewährten Sicherheitsprinzipien (sofern anwendbar) die Anforderungen von 8.3.2c erfüllen,
- c) die Testeinrichtung alle relevanten Fehler erkennt, die nacheinander während des Testablaufs berücksichtigt werden, und eine angemessene Reaktion der Steuerung bewirkt, die:
 - 1) einen sicheren Zustand einleitet, oder wenn das nicht möglich ist,
 - 2) eine Warnung vor der Gefährdung vorsieht.
- d) die mit der Testeinrichtung durchgeführten Prüfungen nicht in einen unsicheren Zustand führen;
- e) die Einleitung der Prüfung durchgeführt wird:
 - 1) beim Maschinenstart und vor der Einleitung einer gefährlichen Situation, und
 - 2) periodisch während des Betriebs, wenn die Risikobeurteilung und die Art des Betriebes zeigen, daß dies notwendig ist.

8.3.4 Kategorie 3

Die sicherheitsbezogenen Teile von Steuerungen müssen nach Kategorie 3 validiert werden, um aufzuzeigen, daß:

- a) sie die Anforderungen der Kategorie B erfüllen,
- b) die bewährten Sicherheitsprinzipien (wenn anwendbar) die Anforderungen von 8.3.2c erfüllen,
- c) ein Einzelfehler nicht zum Verlust der Sicherheitsfunktion führt,
- d) Einzelfehler in Übereinstimmung mit der sinnvollen Gestaltung erkannt werden.

8.3.5 Kategorie 4

Sicherheitsbezogene Teile von Steuerungen der Kategorie 4 müssen validiert werden, um aufzuzeigen, daß:

- a) sie die Anforderungen der Kategorie B erfüllen,
- b) die bewährten Sicherheitsprinzipien (wenn anwendbar) die Anforderungen von 8.3.2c erfüllen,
- c) ein Einzelfehler nicht zum Verlust der Sicherheitsfunktion führt,
- d) die Einzelfehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden,
- e) wenn d) nicht möglich ist, eine Anhäufung von Fehlern nicht zum Verlust der Sicherheitsfunktion(en) führt. Die in Betracht gezogene Erweiterung der Anhäufung von Fehlern muß in Übereinstimmung mit der sinnvollen Gestaltung sein.

8.4 Validierung der Kombination von sicherheitsbezogenen Teilen

Wo die Sicherheitsfunktion durch zwei oder mehrere sicherheitsbezogene Teile ausgeführt ist, muß die Validierung der Kombination (durch Analyse und wenn nötig durch Prüfung) durchgeführt werden, um zu bestätigen, daß die Kombination die in der Gestaltung festgelegte Leistungsfähigkeit erreicht.

9 Validierung der Umgebungsanforderungen

Die in der Gestaltung festgelegte Leistungsfähigkeit von sicherheitsbezogenen Teilen der Steuerung muß validiert werden mit Rücksicht auf die festgelegten Umgebungsbedingungen für die Steuerung.

Die Validierung muß durch Analyse durchgeführt werden und wenn nötig und möglich durch Prüfung. Die Erweiterung der Analyse und Prüfung hängt ab von den sicherheitsbezogenen Teilen, dem System, in dem sie eingebaut sind, der angewandten Technologie und den Umgebungsbedingungen, die validiert werden. Die Anwendung von Betriebszuverlässigkeitsdaten des Systems oder seiner Bauteile, oder die Bestätigung der Übereinstimmung mit den entsprechenden Umgebungsnormen (z. B. für die Wasserdichtigkeit, Vibrationsschutz) können den Validierungsprozeß unterstützen.

Wo anwendbar, muß sich die Validierung beziehen auf:

- zu erwartende mechanische Beanspruchungen durch Schock, Vibration, das Eindringen von Kontaminaten;
- mechanische Haltbarkeit;
- elektrische Nennwerte und Energieversorgungen;
- klimatische Bedingungen (Temperatur und Feuchtigkeit);
- elektromagnetische Verträglichkeit (Immunität).

Wenn es durch die Prüfung notwendig ist, die Übereinstimmung mit den Umgebungsanforderungen zu bestimmen, müssen die Vorgehensweisen, wie sie in den entsprechenden Normen beschrieben sind, befolgt werden, soweit es für die Anwendung erforderlich ist.

Nach der gesamten Durchführung der Validierung durch Prüfung müssen die Sicherheitsfunktionen ferner in Übereinstimmung mit den Festlegungen für die sicherheitstechnischen Anforderungen sein, oder die Ausgänge sicherheitsbezogener Teile müssen für einen sicheren Zustand sorgen.

10 Validierung der Instandhaltungsanforderungen

Das Validierungsverfahren muß durch Analyse aufzeigen, daß die Instandhaltungsanforderungen wie sie in EN 954-1:1996, Abschnitt 9, Absatz 2, festgelegt sind, einbezogen wurden.

Anhang A (informativ)

Möglichkeiten zur Validierung mechnischer Systeme

Inhalt

Seite

A.0 Einleitung	16
A.1 Liste der grundlegenden Sicherheitsprinzipien	17
Tabelle A.1: Grundlegende Sicherheitsprinzipien	17
A.2 Liste der bewährten Sicherheitprinzipien	18
Tabelle A.2: Bewährte Sicherheitsprinzipien	18
A.3 Liste der bewährten Bauteile	19
Tabelle A.3: Bewährte Bauteile	20
A.4 Fehlerlisten und Fehlerausschlüsse	20
A.4.0 Einleitung	20
A.4.1 Verschiedene mechanische Geräte, Bauteile und Elemente	21
Tabelle A.4: Mechanische Geräte, Bauteile und Elemente	21
A.4.2 Druckfedern	21
Tabelle A.5: Druckfedern	21

A.0 Einleitung

Bei Anwendung mechanischer Systeme in Verbindung mit anderen Technologien sollten auch die zutreffenden Tabellen für grundlegende und bewährte Sicherheitsprinzipien berücksichtigt werden.

A.1 Liste der grundlegenden Sicherheitsprinzipien

Tabelle A.1: Grundlegende Sicherheitsprinzipien

Grundlegende Sicherheitsprinzipien	Bemerkungen
Anwendung geeigneter Werkstoffe und Herstellungsverfahren	Auswahl des Werkstoffs, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von (z. B. Spannungen, Haltbarkeit, Elastizität, Reibung, Verschleiß, Korrosion, Temperatur) .
Richtige Dimensionierung und Formgebung	Berücksichtigen (z. B. von Spannung, Dehnung, Ermüdung, Oberflächenrauheit, Toleranzen, Hängenbleiben, ..
Geeignete Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau der Bauteile/des Systems	Berücksichtigen von Anwendungshinweisen des Herstellers (z. B. Katalogblätter, Einbauanweisungen, Festlegungen) sowie Erfahrungen mit ähnlichen Bauteilen/Systemen .
Anwendung des Ausschaltprinzips	Der sichere Zustand wird durch Abtrennung von der Energiequelle erreicht. Siehe Primärmaßnahme zur Außerbetriebnahme in EN 292-2 : 1991, 3.7.1. Zum Starten der Bewegung eines Mechanismus wird Energie benötigt. Siehe Primärmaßnahme zur Inbetriebnahme in EN 292-2 : 1991, 3.7.1. Berücksichtigen von unterschiedlichen Betriebsarten (z. B. Betriebsmodus, Wartungsmodus). In Sonderfällen können Ausnahmen möglich sein (z. B. Beibehaltung der Energie für Spanneinrichtungen). In diesem Fall sollte ein Warnzeichen an der Maschine gegeben werden.
Geeignete Befestigung	Zur Anwendung von Schraubensicherungen beachten der Anwendungshinweise des Herstellers. Die Anwendung des richtigen Drehmoments ist die Voraussetzung dafür, daß Schrauben ohne Überlastung festgezogen werden.
Begrenzung der Kraft und ähnlicher Parameter	Beispiele sind Abscherstift, Abscherblech, Drehmomentenkupplung.
Begrenzung der Geschwindigkeit und ähnlicher Parameter	Diese Parameter sind z. B. Temperatur, Feuchtigkeit, Verunreinigungen am Einbauort. Siehe Abschnitt 9 und Anwendungshinweise des Herstellers beachten.
Geeignete Reaktionszeit	Beachten von z. B. Verringerung der Federkraft, Reibung, Schmierung, Temperatur, Trägheit bei Beschleunigung und Verzögerung, Kombination von Toleranzen.
Schutz gegen unerwartetem Anlauf	Berücksichtigen von unerwartetem Anlauf, der durch gespeicherte Energie und nach Wiederherstellung der Energieversorgung verursacht wird, für unterschiedliche Betriebsarten, wie Betriebsmodus, Wartungsmodus usw. Eine besondere Einrichtung zum Abtrennen der gespeicherten Energie kann erforderlich sein. In Sonderfällen können Ausnahmen möglich sein (z. B. Beibehaltung der Energie für Spanneinrichtungen).

(fortgesetzt)

Tabelle A.1 (abgeschlossen)

Grundlegende Sicherheitsprinzipien	Bemerkungen
Vereinfachung	Verringern der Anzahl der Bauteile in sicherheitsbezogenen Systemen. Trennen der sicherheitsbezogenen Funktionen von anderen Funktionen.

A.2 Liste der bewährten Sicherheitsprinzipien

Tabelle A.2: Bewährte Sicherheitsprinzipien

Bewährte Sicherheitsprinzipien	Bemerkungen
Anwendung sorgfältig ausgewählter Werkstoffe und Herstellungsverfahren	Auswahl der für die jeweilige Anwendung geeigneten Werkstoffe sowie zweckdienlicher Herstellungs- und Behandlungsverfahren.
Anwendung von Bauteilen mit gerichteter Ausfallart	Die überwiegend auftretende Ausfallart eines Bauteils ist im voraus bekannt und stets die gleiche, siehe EN 292-2 : 1991, 3.7.4.
Überdimensionierung/Sicherheitsfaktor	Die Sicherheitsfaktoren werden in Vorschriften oder Normen angegeben oder beruhen auf Erfahrungen mit sicherheitsbezogenen Anwendungen.
Bistabiler Betrieb	Das bewegliche Element eines Bauteils wird mechanisch in beiden möglichen Positionen befestigt (Reibung allein ist nicht ausreichend). Um die Position zu verändern, ist das Aufbringen von Druck/Kraft notwendig.
Erhöhte AUS-Kraft	Eine sichere Position/ein sicherer Zustand wird dadurch erreicht, daß die AUS-Kraft gegenüber der EIN-Kraft erhöht wird (Sicherheitsfaktor).
Sorgfältige Auswahl, Kombination, Anordnung, Zusammenbau und Einbau von Bauteilen/Systemen für die jeweilige Anwendung	–
Sorgfältige Auswahl der Befestigungsart für die jeweilige Anwendung	–
Zwangsläufige mechanische Funktion	Der abhängige Betrieb (z. B. Parallelbetrieb) mehrerer Teile wird durch ein mechanisches Verbindungsglied (oder mehrere) erreicht. Das/die Verbindungsglied(er) sollten keine Federn und ähnliche "flexible" Elemente enthalten.
Mehrfachanwendung gleicher Teile	Verringerung der Fehlerwirkung durch Mehrfachanwendung gleicher Teile, wobei z. B. ein Fehler, der an einer Feder (von vielen Federn) auftritt, keinen gefährlichen Zustand bewirkt.

(fortgesetzt)

Tabelle A.2 (abgeschlossen)

Bewährte Sicherheitsprinzipien	Bemerkungen
Anwendung bewährter Federn (siehe auch Tabelle A.3)	Bei Bemessung einer bewährten Feder erfordert: – Anwendung sorgfältig ausgewählter Werkstoffe, Herstellungsverfahren (z. B. vor Anwendung vorgenommene Voreinstellungen und periodische Wiederholungen) und Behandlungsverfahren (z. B. Walzen und Kugelstrahlen); – ausreichende Führung der Feder und – ausreichender Sicherheitsfaktor bei Dauerbeanspruchung (d. h. mit hoher Wahrscheinlichkeit tritt kein Bruch auf). Bewährte Spiraldruckfedern dürfen auch bemessen werden durch: – Anwendung sorgfältig ausgewählter Werkstoffe, Herstellungsverfahren (z. B. vor Anwendung vorgenommene Voreinstellungen und periodische Wiederholungen) und Behandlungsverfahren (z. B. Walzen und Kugelstrahlen); – ausreichende Federführung und – eines Spiels zwischen den Windungen, das kleiner als der Drahtdurchmesser der unbelasteten Feder ist, und – einer ausreichenden Kraft nach einem Bruch oder nach mehreren Brüchen (d. h. ein Bruch führt nicht zu einem gefährlichen Zustand).
Bereichsbegrenzung der Kraft und ähnlicher Parameter	Festlegen der notwendigen Begrenzung in Abhängigkeit von Erfahrungen und der jeweiligen Anwendung. Beispiele für Begrenzungen sind Abscherstift, Abscherblech, Drehmomentenkupplung.
Bereichsbegrenzung der Geschwindigkeit und ähnlicher Parameter	Festlegen der notwendigen Begrenzung in Abhängigkeit von Erfahrungen und der jeweiligen Anwendung. Beispiele für Begrenzungen sind Fliehkraftregler usw.
Bereichsbegrenzung der Umgebungsparameter	Festlegen der notwendigen Begrenzungen. Beispiele für diese Parameter sind Temperatur, Feuchtigkeit, Verunreinigung beim Einbau. Siehe Abschnitt 9 und Anwendungshinweise der Hersteller beachten.
Bereichsbegrenzung der Reaktionszeit Hysteresebegrenzung	Festlegen der notwendigen Begrenzungen. Beachten von z. B. Verringerung der Federkraft, Reibung, Schmierung, Temperatur, Trägheit bei Beschleunigung und Verzögerung, Kombination von Toleranzen

A.3 Liste der bewährten Bauteile

Die in der folgenden Liste aufgeführten bewährten Bauteile für sicherheitsbezogene Anwendungen beruhen auf der Anwendung von bewährten Sicherheitsprinzipien und/oder einer Norm für deren spezielle Anwendungen.

Ein für bestimmte Anwendungen „bewährtes Bauteil“ kann für andere Anwendungen ungeeignet sein.

Tabelle A.3: Bewährte Bauteile

Bauteile	Bedingungen für „bewährt“	Norm oder Spezifikation
Schraube	Alle Faktoren, die auf die Schraubverbindung und die Anwendung einen Einfluß ausüben, sind zu berücksichtigen Siehe A.2 „Liste bewährter Sicherheitsprinzipien“	Mechanische Verbindungselemente, wie Schrauben, Muttern, Unterlegescheiben, Nieten usw. sind in verschiedenen EN- und EN ISO-Normen festgelegt. Beiblatt 3 zu DIN 918:1999 enthält einen Überblick über diese Normen.
Feder	Siehe A.2 „Anwendung bewährter Federn“	Technische Festlegungen für Federstähle und andere Sonderanwendungsfälle sind in ISO/DIS 4960 zu finden.
Nocken	Alle Faktoren, die auf die Anordnung des Nockens (z. B. als Teil einer Verriegelung) Einfluß nehmen, sind zu berücksichtigen. Siehe A.2 "Liste bewährter Sicherheitsprinzipien"	Siehe EN 1088 (Verriegelungen).
Abscherstift	Alle Faktoren, die auf die Anwendung Einfluß nehmen, sind zu berücksichtigen. Siehe A.2 "Anwendung bewährter Sicherheitsprinzipien"	

A.4 Fehlerlisten und der Fehlerausschlüsse

A.4.0 Einleitung

In den Listen werden einige Fehlerausschlüsse und die dazugehörigen Begründungen angegeben. Weitere begründete Ausschlüsse können zulässig sein (z. B. bei einer geringen Fehlerwahrscheinlichkeit).

Bei der Validierung sollten sowohl dauernd als auch nicht dauernd auftretende Fehler berücksichtigt werden.

Der exakte Moment, in dem der Fehler auftritt, kann kritisch sein. Durch eine theoretische Fehleruntersuchung sollte der ungünstigste Fall ermittelt werden (z. B. im Stillstand, während des Anfahrens oder während des Betriebs des Systems). Die Prüfung sollte im voraus durchgeführt werden.

A.4.1 Verschiedene mechanische Geräte, Bauteile und Elemente

Tabelle A.4: Mechanische Geräte, Bauteile und Elemente
z. B. Nocken, Stößel, Kette, Kupplung, Bremse, Welle, Schraube, Stift, Führung, Lager

Angenommener Fehler	Fehlerausschluß	Bemerkungen
Verschleiß/Korrosion	Ja, wenn Werkstoff, (Über-)Dimensionierung, Herstellungs-, Behandlungsverfahren und geeignete Schmierung entsprechend der vorgesehenen Lebensdauer sorgfältig ausgewählt werden (siehe auch Tabelle A.2).	Siehe EN 954-1:1996, 7.2
Nicht Festziehen/Lösen	Ja, wenn Werkstoff, Herstellungs-, Behandlungsverfahren entsprechend der vorgesehenen Lebensdauer sorgfältig ausgewählt werden (siehe auch Tabelle A.2).	
Bruch	Ja, wenn Werkstoff, (Über-)Dimensionierung, Herstellungs-, Behandlungsverfahren und geeignete Schmierung entsprechend der vorgesehenen Lebensdauer sorgfältig ausgewählt werden (siehe auch Tabelle A.2).	
Verformung und Überbeanspruchung	Ja, wenn Werkstoff, (Über-)Dimensionierung, Herstellungs-, Behandlungsverfahren und geeignete Schmierung entsprechend der vorgesehenen Lebensdauer sorgfältig ausgewählt werden (siehe auch Tabelle A.2).	
Steifheit/Hängenbleiben	Ja, wenn Werkstoff, (Über-)Dimensionierung, Herstellungs-, Behandlungsverfahren und geeignete Schmierung entsprechend der vorgesehenen Lebensdauer sorgfältig ausgewählt werden (siehe auch Tabelle A.2).	

A.4.2 Druckfedern

Tabelle A.5: Druckfedern

Angenommener Fehler	Fehlerausschluß	Bemerkungen
Verschleiß/Korrosion	Siehe Tabelle A.2 „Anwendung bewährter Federn“	Siehe EN 954-1:1996, 7.2
Verringerung der Kraft durch bleibende Verformung und Bruch		
Bruch		
Steifheit/Hängenbleiben		
Lösen		
Verformung durch Überbeanspruchung		

Anhang B (informativ)

Möglichkeiten zur Validierung pneumatischer Systeme

Inhalt

	Seite
B.0 Einleitung	22
B.1 Liste der grundlegenden Sicherheitsprinzipien	23
Tabelle B.1: Grundlegende Sicherheitsprinzipien	23
B.2 Liste der bewährten Sicherheitsprinzipien	25
Tabelle B.2: Bewährte Sicherheitsprinzipien	25
B.3 Liste der bewährten Bauteile	26
Tabelle B.3: (leer)	26
B.4 Fehlerlisten und Fehlerausschlüsse	26
B.4.0 Einleitung	26
B.4.1 Ventile	26
Tabelle B.4: Wegeventile	26
Tabelle B.5: Sperrventile (Absperrventile)	28
Tabelle B.6: Stromventile	29
Tabelle B.7: Druckventile	30
B.4.2 Leitungen	31
Tabelle B.8: Rohrleitungen	31
Tabelle B.9: Schlauchleitungen	32
Tabelle B.10: Verbindungselemente	32
B.4.3 Druckübersetzer /Druckmittelwandler	33
Tabelle B.11: Druckübersetzer/Druckmittelwandler	33
B.4.4 Druckluftaufbereitung	33
Tabelle B.12: Filter	33
Tabelle B.13: Öler	34
Tabelle B.14: Schalldämpfer	34
B.4.5 Energiespeicher und Druckbehälter	35
Tabelle B.15: Energiespeicher und Druckbehälter	35
B.4.6 Sensoren	35
Tabelle B.16: Sensoren	35
B.4.7 Informationsverarbeitung	35
Tabelle B.17: Verknüpfungsglieder	35
Tabelle B.18: Verzögerungsglieder	36
Tabelle B.19: Umformer	36

B.0 Einleitung

Bei Anwendung pneumatischer Systeme in Verbindung mit anderen Technologien sollten auch die zutreffenden Tabellen für grundlegende und bewährte Sicherheitsprinzipien berücksichtigt werden. Wo Ventile elektrisch angesteuert werden, sollten die entsprechenden Fehlerlisten im Anhang D berücksichtigt werden.

B.1 Liste der grundlegenden Sicherheitsprinzipien

Tabelle B.1: Grundlegende Sicherheitsprinzipien

Grundlegende Sicherheitsprinzipien	Bemerkungen
Anwendung geeigneter Werkstoffe und Herstellungsverfahren	Auswahl des Werkstoffs, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von z. B. Spannungen, Haltbarkeit, Elastizität, Reibung, Verschleiß, Korrosion, Temperatur.
Richtige Dimensionierung und Formgebung	Berücksichtigen z. B. von Spannungen, Dehnungen, Ermüdung, Oberflächenrauheit, Toleranzen, Hängenbleiben, Herstellung.
Geeignete Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau der Bauteile/ des Systems	Berücksichtigen von Anwendungshinweisen des Herstellers (z. B. Katalogblätter, Einbauanweisungen, Festlegungen) sowie von Erfahrungen mit ähnlichen Bauteilen/Systemen.
Anwendung des Prinzips der Energietrennung	Der sichere Zustand wird erreicht, indem alle wichtigen Einrichtungen von der Energiequelle abgetrennt werden. Siehe Primärmaßnahmen zum Anhalten in EN 292-2 : 1991, 3.7.1. Zum Starten der Bewegung eines Mechanismus wird Energie benötigt. Siehe Primärmaßnahmen zum Starten in EN 292-2 : 1991, 3.7.1. Berücksichtigen von unterschiedlichen Betriebsarten (z. B. Betriebsmodus, Wartungsmodus). In Sonderfällen können Ausnahmen möglich sein (z. B. wenn der Ausfall der pneumatischen Energie eine zusätzliche Gefährdung erzeugt).
Geeignete Befestigung	Zur Anwendung von z. B. Schraubensicherungen, Armaturen, Klebungen, Spannrings beachten der Anwendungshinweise des Herstellers. Die Anwendung des richtigen Drehmoments ist die Voraussetzung für: a) das Festziehen und b) die Nichtüberbelastung von Schrauben und Armaturen.
Druckbegrenzung	Beispiele sind Überdruckventile, Druckminder-/ Druckregelventile.
Begrenzung/Verringerung der Geschwindigkeit	Ein Beispiel ist die Geschwindigkeitsbegrenzung eines Kolbens durch ein Stromventil oder eine Drossel.
Ausreichende Maßnahmen zur Vermeidung von Verunreinigung des Druckmediums	Berücksichtigen von Filtration des Druckmediums/ Abtrennung von Feststoffen und Wasser.
Geeigneter Schaltzeitbereich	Berücksichtigen von z. B. der Länge der Rohrleitung, Druck, Entlüftungskapazität, Kraft, Verringerung der Federkraft, Reibung, Schmierung, Temperatur, Trägheit bei Beschleunigung und Verzögerung, Zusammenwirken von Toleranzen.
Beständigkeit gegen Umgebungsbedingungen	Gestalten der Einrichtung, daß sie in allen für den Einsatz zu erwartenden Umgebungen und in allen vorhersehbaren ungünstigen Bedingungen (z. B. für Temperatur, Feuchtigkeit, Schwingungen, Verunreinigungen) arbeitet. Siehe Abschnitt 9 und Spezifikationen/Anwendungshinweise des Herstellers beachten.

(fortgesetzt)

Tabelle B.1 (abgeschlossen)

Grundlegende Sicherheitsprinzipien	Bemerkungen
Schutz gegen unerwarteten Anlauf	Berücksichtigen von unerwartetem Anlauf, verursacht durch gespeicherte Energie und nach Wiederherstellung der Energieversorgung, für unterschiedliche Betriebsarten, (z. B. Betriebsmodus, Wartungsmodus). Ein besonderes Gerät zum Ablassen der gespeicherten Energie kann erforderlich sein. In Sonderfällen können Ausnahmen möglich sein (z. B. Beibehaltung der Energie für Spanneinrichtungen). In diesem Fall sollte ein Warnzeichen an der Maschine gegeben werden.
Vereinfachung	Verringern der Anzahl der Bauteile in sicherheitsbezogenen Systemen Trennen der sicherheitsbezogenen Funktionen von anderen Funktionen.

B.2 Liste der bewährten Sicherheitsprinzipien

Tabelle B.2: Bewährte Sicherheitsprinzipien

Bewährte Sicherheitsprinzipien	Bemerkungen
Überdimensionierung/Sicherheitsfaktor	Die Sicherheitsfaktoren werden in Vorschriften oder Normen angegeben oder beruhen auf Erfahrungen mit sicherheitsbezogenen Anwendungen.
Bistabiler Betrieb	Das bewegliche Element eines Bauteils wird mechanisch in einer der beiden möglichen Positionen fixiert (Reibung allein ist nicht ausreichend). Um die Position zu verändern, ist das Aufbringen von Druck/Kraft notwendig.
Überdimensionierung der AUS-Kraft gegenüber der EIN-Kraft	Eine Lösung kann sein, daß das Flächenverhältnis für die Bewegung des Ventilkolbens in die sichere Position (AUS-Stellung) gegenüber dem Flächenverhältnis für die Bewegung des Ventilkolbens in die EIN-Stellung deutlich größer ist (ein Sicherheitsfaktor).
Durch den Lastdruck selbstschließendes Ventil	Beispiele sind Ventile in Sitz- und Patronen-Bauart. Berücksichtigen, wie der Druck aufzubringen ist, um das Ventil auch dann geschlossen zu halten, wenn z. B. die Schließfeder des Ventils bricht.
Zwangsläufige mechanische Wirkung/Betätigung	Die zwangsläufige mechanische Wirkung/Betätigung wird für die bewegten Teile in pneumatischen Bauteilen angewendet, siehe auch Tabelle A.2.
Vervielfachung von Teilen	Siehe Tabelle A.2.
Bewährte Feder	Siehe Tabelle A.2
Begrenzung/Verringerung der Geschwindigkeit durch Widerstand zum Erreichen eines konstanten Volumenstroms	Beispiele sind Festblende, Festdrossel.
Begrenzung/Verringerung der Kraft durch bewährtes Druckbegrenzungsventil	Ein bewährtes Druckbegrenzungsventil enthält z. B. eine bewährte Feder.
Geeigneter Bereich für die Betriebsbedingungen	Die Eingrenzung der Betriebsbedingungen, z. B. Druck-, Volumenstrom- und Temperaturbereich, sollte berücksichtigt werden.
Geeignetes Vermeiden einer Verunreinigung des Druckmediums	Berücksichtigen von hoch wirksamer Filtration des Druckmediums/Abscheidung von Feststoffen und Wasser.
Ausreichend große positive Überdeckung in sSchieberventilen	Die positive Überdeckung sichert die Stopp-Funktion und verhindert unzulässige Bewegungen.
Hysteresebegrenzung	Die Hysteresis erhöht sich z. B. durch stärkere Reibung. Kombination von Toleranzen beeinflußt die Hysteresis ebenfalls.

B.3 Liste der bewährten Bauteile

Eine Liste von bewährten Bauteilen wird nicht gegeben. Bauteile dürfen als bewährt bezeichnet werden, falls sie den in EN 954-1:1996, 6.2.2 und in EN 983:1996, Abschnitte 5 bis 7 angegebenen Beschreibungen entsprechen.

Ein für bestimmte Anwendungen „bewährtes Bauteil“ kann für andere Anwendungen ungeeignet sein.

Tabelle B.3: (leer)

B.4 Fehlerlisten und Fehlerausschlüsse

B.4.0 Einleitung

In den Listen werden einige Fehlerausschlüsse und die zugehörigen Begründungen angegeben. Weitere begründete Ausschlüsse können zulässig sein (z. B. bei einer geringen Fehlerwahrscheinlichkeit).

Bei der Validierung sollten sowohl dauernd als auch nicht dauernd auftretende Fehler berücksichtigt werden.

Der exakte Moment, in dem der Fehler auftritt, kann kritisch sein. Durch eine theoretische Fehleruntersuchung sollte der ungünstigste Fall ermittelt werden (z. B. im Stillstand, während des Anfahrens oder während des Betriebs des Systems). Die Prüfung sollte im voraus durchgeführt werden.

B.4.1 Ventile

Tabelle B.4: Wegeventile

Fehlerannahme	Fehlerausschluß	Bemerkungen
Veränderung der Schaltzeiten	Ja, bei zwangsläufiger mechanischer Betätigung (siehe Tabelle A.2) der bewegten Bauteile, sofern die Betätigungskraft ausreichend groß ist.	
Nichtschalten (Hängenbleiben in einer End- oder Nullage) oder nicht vollständiges Schalten (Hängenbleiben in einer beliebigen Zwischenstellung)	Ja, bei zwangsläufiger mechanischer Betätigung (siehe Tabelle A.2) der bewegten Bauteile, sofern die Betätigungskraft ausreichend groß ist.	
Selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal)	Ja, bei zwangsläufiger mechanischer Betätigung (siehe Tabelle A.2) der bewegten Bauteile, sofern die Haltekraft ausreichend groß ist. Ja, wenn bewährte Federn angewendet werden (siehe Tabelle A.2) und wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung 1)). Ja, bei Schieberventilen mit elastischer Abdichtung und wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung 1)).	1) Übliche Einbau- und Betriebsbedingungen liegen vor, wenn: – die vom Hersteller vorgegebenen Bedingungen eingehalten werden; – sich die Gewichtskraft des bewegten Bauteils sicherheitstechnisch nicht ungünstig auswirkt (z. B. horizontaler Einbau); – keine besonderen Massenträgheitskräfte auf die bewegten Bauteile wirken (z. B. Beachtung der Bewegungsrichtung bei Anordnung auf bewegten Maschinenteilen) und – keine extremen Schwingungs- und Schockbeanspruchungen auftreten.

(fortgesetzt)

Tabelle B.4 (abgeschlossen)

Fehlerannahme	Fehlerausschluß	Bemerkungen
Leckage	Ja, bei Schieberventilen mit elastischer Abdichtung, sofern eine ausreichende positive Überdeckung vorhanden ist (siehe Bemerkung 2)), und wenn übliche Betriebsbedingungen vorliegen und die Druckluft ausreichend aufbereitet und filtriert wird. Ja, bei Sitzventilen, wenn übliche Betriebsbedingungen vorliegen und die Druckluft ausreichend aufbereitet und filtriert wird.	2) Bei Schieberventilen mit elastischer Abdichtung können Effekte durch eine Leckage in der Regel ausgeschlossen werden. Über eine längere Dauer kann jedoch eine geringe Leckage auftreten.
Veränderung des Leckagevolumenstroms über eine längere Dauer	Nein	
Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben	Ja, wenn Konstruktion, Dimensionierung und Einbau den Regeln der Technik entsprechen.	
Für Servo- und Proportionalventile: Pneumatische Fehler, die unkontrolliertes Verhalten bewirken	Ja, bei Servo- und Proportionalwegeventilen, wenn sie bedingt durch ihre konstruktive Ausführung sicherheitstechnisch wie konventionelle Wegeventile beurteilt werden können.	
ANMERKUNG: Werden Ventilfunktionen (Schaltsymbole) durch die Funktionen mehrerer Bauteile (Einzelventile) realisiert, sollte eine Fehlerbetrachtung für jedes einzelne bewegte Bauteil durchgeführt werden. Bei vorgesteuerten Ventilen ist entsprechend vorzugehen.		

Tabelle B.5: Sperrventile (Absperrventile)
(z. B. Rückschlag-, Schnellentlüftungs- und Wechselventile)

Fehlerannahme	Fehlerausschluß	Bemerkungen
Veränderung der Schaltzeiten	Nein	
Nichtöffnen, nicht vollständiges Öffnen, Nichtschließen sowie nicht vollständiges Schließen (Hängenbleiben in einer Endlage oder in einer beliebigen Zwischenstellung)	Ja, wenn die Führungsverhältnisse für das/die bewegte(n) Bauteil(e) etwa denen eines nicht gesteuerten Kugelsitzventils ohne Dämpfungssystem entsprechen (siehe Bemerkung 1)) und wenn bewährte Federn angewendet werden (siehe Tabelle A.2).	1) Für ein nicht gesteuertes Kugelsitzventil ohne Dämpfungssystem sind die Führungsverhältnisse im allgemeinen so gestaltet, daß ein Hängenbleiben hinreichend unwahrscheinlich ist.
Selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal)	Ja, wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung 2)) und eine ausreichende Schließkraft aufgrund der vorliegenden Druck- und Flächenverhältnisse vorhanden ist.	2) Übliche Einbau- und Betriebsbedingungen liegen vor, wenn: – die vom Hersteller festgelegten Bedingungen eingehalten werden; – keine besonderen Massenträgheitskräfte auf die bewegten Bauteile wirken, z. B. Beachtung der Bewegungsrichtung bei Anordnung auf bewegten Maschinenteilen, und – keine extremen Schwingungs- und Schockbeanspruchungen auftreten.
Für Wechselventile: gleichzeitiger Verschluß beider Eingangsanschlüsse	Ja, wenn bedingt durch Konstruktion und Ausführung des bewegten Bauteils der gleichzeitige Verschluß hinreichend unwahrscheinlich ist.	
Leckage	Ja, wenn übliche Betriebsbedingungen vorliegen und die Druckluft ausreichend aufbereitet und filtriert wird.	
Veränderung des Leckagevolumenstroms über eine längere Dauer	Nein	
Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben	Ja, wenn Konstruktion, Dimensionierung und Einbau den Regeln der Technik entsprechen.	

Tabelle B.6: Stromventile

Fehlerannahme	Fehlerausschluß	Bemerkungen
Veränderung des Volumenstroms ohne Veränderung der Verstelleinrichtung	Ja, bei Stromventilen ohne bewegte Teile (siehe Bemerkung 1)), z. B. Drosselventile, wenn übliche Betriebsbedingungen vorliegen (siehe Bemerkung 2)) und die Druckluft ausreichend aufbereitet und filtriert wird.	1) Die Verstelleinrichtung wird nicht als bewegtes Bauteil betrachtet. Veränderungen des Volumenstroms durch Änderung der Druckdifferenz sind bei diesem Ventiltyp physikalisch bedingt und nicht Gegenstand dieser Fehlerannahme. 2) Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen eingehalten werden.
Veränderung des Volumenstroms bei nicht einstellbaren, kreisförmigen Blenden und Düsen	Ja, wenn der Durchmesser $\geq 0,8$ mm ist, übliche Betriebsbedingungen vorliegen (siehe Bemerkung 2)) und die Druckluft ausreichend aufbereitet und filtriert wird.	
Bei Proportionalstromventilen: Veränderung des Volumenstroms durch unbeabsichtigte Veränderung des Einstellwertes	Nein	
Selbsttätige Veränderung der Verstelleinrichtung	Ja, bei einer wirksamen und dem Einsatzfall angepaßten Sicherung der Verstelleinrichtung unter Beachtung sicherheitstechnischer Festlegungen, z. B. Plombierung.	
Unbeabsichtigtes Lösen des Stellteils/der Stellteile der Verstelleinrichtung	Ja, wenn eine wirksame formschlüssige Sicherung gegen das Lösen vorhanden ist.	
Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben	Ja, wenn Konstruktion, Dimensionierung und Einbau den Regeln der Technik entsprechen.	

Tabelle B.7: Druckventile

Fehlerannahme	Fehlerausschluß	Bemerkungen
Nichtöffnen oder nicht ausreichen- des Öffnen (weg- und zeitmäßig) bei Überschreiten des Einstelldruckes	Ja, wenn: – die Führungsverhältnisse für das/die bewegte(n) Bauteil(e) etwa denen eines nicht gesteuerten Kugelsitz- oder Membranventils entsprechen (siehe Bemerkung 2)), z. B. bei einem Druckminderventil mit	1) Diese Fehlerannahme gilt nur, wenn das Druckventil insbesondere für Kraftwirkungen, z. B. zum Spannen, angewandt wird. Diese Fehlerannahme gilt nicht für die übliche Funktion eines Druckventils in Pneumatiksystemen, z. B. Druckminderung, Druckbegrenzung. Sie gilt nicht für den vorgesehenen Anwen- dungsbereich typgeprüfter Druck- begrenzungsventile.
Nichtschließen oder nicht voll- ständiges Schließen (weg- und zeitmäßig) bei Unterschreiten des Einstelldruckes (Hängenbleiben oder Schwergängigkeit des bewegten Bauteils) (siehe Bemerkung 1))	Sekundärdruckbegrenzung und – die eingebaute(n) Feder(n) bewährte Feder(n) sind (siehe Tabelle A.2).	
Veränderung des Druck-Regel- verhaltens ohne Veränderung der Verstelleinrichtung (siehe Bemerkung 1))	Ja, bei direkt betätigten Druckbegren- zungsventilen sowie Druckschaltventilen, wenn (eine) bewährte Feder(n) ein- gebaut ist/sind (siehe Tabelle A.2).	2) Für ein nicht gesteuertes Kugel- sitz- oder Membranventil ist das Führungsverhältnis im allgemeinen so gestaltet, daß ein Hängen- bleiben des bewegten Bauteils hinreichend unwahrscheinlich ist.
Für Proportional-Druckventile: Veränderung des Druck-Regelver- haltens durch unbeabsichtigte Ver- änderung des Einstellwertes (siehe Bemerkung 1))	Nein	
Selbsttätige Veränderung der Verstelleinrichtung	Ja, bei einer wirksamen und dem Ein- satzfall angepaßten Sicherung der Ver- stelleinrichtung unter Beachtung sicherheitstechnischer Festlegungen, z. B. Plombierung.	
Unbeabsichtigtes Herausdrehen des Stellteils der Verstellein- richtung	Ja, wenn eine wirksame formschlüssige Sicherung gegen das Herausdrehen vorhanden ist.	
Leckage	Ja, für Sitzventile, Membranventile und Schieberventile mit elastischer Abdichtung, bei üblichen Be- triebsbedingungen (siehe Bemerkung 3)) und wenn die Druckluft ausreichend aufbereitet und filtriert wird.	3) Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedin- gungen eingehalten wurden.
Veränderung des Leckagevolumenstroms über eine längere Dauer	Nein	
Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben	Ja, wenn Konstruktion, Dimensionierung und Einbau den Regeln der Technik entsprechen.	

B.4.2 Leitungen

Tabelle B.8: Rohrleitungen

Fehlerannahme	Fehlerausschluß	Bemerkungen
Bersten und Leckage	Ja, wenn Dimensionierung, Auswahl der Werkstoffe und Befestigung den Regeln der Technik entsprechen (siehe Bemerkung 1)).	1) Bei Anwendung von Kunststoffrohren sind die Herstellerangaben zu beachten, insbesondere bezüglich der Umgebungseinflüsse während des Betriebs, z. B. thermische Einflüsse, chemische Einflüsse, Einflüsse durch Strahlung. Bei Anwendung von Stahlrohren, die nicht mit einem korrosionshemmenden Mittel behandelt wurden, ist es besonders wichtig, die Druckluft ausreichend zu trocknen.
Abreißen am Verbindungselement und Leckage	Ja, wenn Schneidringverschraubungen oder Gewinderohre (d. h. Stahlittings, Stahlrohre) angewendet werden und wenn Dimensionierung, Auswahl der Werkstoffe, Herstellung, Anordnung und Befestigung den Regeln der Technik entsprechen.	
Zusetzen (Verstopfen)	Ja, bei Rohrleitungen im Leistungskreis. Ja, bei Steuer- und Meßleitungen, wenn die Nennweite ≥ 2 mm ist.	
Abknicken von Kunststoffrohren mit geringer Nennweite	Ja, wenn die Rohrleitungen entsprechend geschützt verlegt und die entsprechenden Herstellerangaben berücksichtigt werden, z. B. minimaler Biegeradius.	

Tabelle B.9: Schlauchleitungen

Fehlerannahme	Fehlerausschluß	Bemerkungen
Bersten, Ausreißen aus der Einbindung und Leckage	Ja, wenn Schlauchleitungen aus Schläuchen nach EN 854 oder aus ähnlichen Schläuchen und den zugehörigen Schlaucharmaturen angewendet werden.	
Zusetzen (Verstopfen)	Ja, bei Schlauchleitungen im Leistungskreis. Ja, bei Steuer- und Meßleitungen, wenn die Nennweite ≥ 2 mm ist.	

Tabelle B.10: Verbindungselemente

Fehlerannahme	Fehlerausschluß	Bemerkungen
Bersten, Schraubenbruch oder Ausreißen der Gewinde	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Herstellung, Anordnung und Verbindung zur Leitung und/oder zu den fluidtechnischen Bauteilen den Regeln der Technik entsprechen.	
Leckage (Versagen der Dichtwirkung)	Nein	
Zusetzen (Verstopfen)	Ja, bei Anwendungen im Leistungskreis. Ja, bei Steuer- und Meßleitungen, wenn die Nennweite ≥ 2 mm ist.	

B.4.3 Druckübersetzer/Druckmittelwandler

Tabelle B.11: Druckübersetzer/Druckmittelwandler

Fehlerannahme	Fehlerausschluß	Bemerkungen
Verlust oder Veränderung der Dichtwirkung der Druckräume	Nein	
Bersten der Druckräume sowie Bruch von Befestigungs- oder Deckelschrauben	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Anordnung und Befestigung den Regeln der Technik entsprechen (siehe Bemerkung 1)).	1) Es könnten auch die Anforderungen der Richtlinien 87/404/EWG und 90/488/EWG für einfache Druckbehälter und der Richtlinie 97/23/EG für Druckgeräte einschließlich der dort erfaßten zutreffenden Regeln zu beachten sein.

B.4.4 Druckluftaufbereitung

Tabelle B.12: Filter

Fehlerannahme	Fehlerausschluß	Bemerkungen
Zusetzen des Filterelements	Nein	
Bruch oder teilweiser Bruch des Filterelements	Ja, wenn das Filterelement eine ausreichende Druckfestigkeit hat.	
Ausfall der Verschmutzungs-Anzeige- oder – Überwachungseinrichtung	Nein	
Bersten des Filtergehäuses oder Bruch der Deckel- oder Verbindungselemente	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Anordnung im System und Befestigung den Regeln der Technik entsprechen (siehe Bemerkung 1)).	1) Es könnten auch die Anforderungen der Richtlinien 87/404/EWG und 90/488/EWG für einfache Druckbehälter und der Richtlinie 97/23/EG für Druckgeräte einschließlich der dort erfaßten zutreffenden Regeln zu beachten sein.

Tabelle B.13: Öler

Fehlerannahme	Fehlerausschluß	Bemerkungen
Veränderung des Einstellwertes (Ölvolumen je Zeiteinheit) ohne Veränderung der Verstelleinrichtung	Nein	
Selbsttätige Veränderung der Verstelleinrichtung	Ja, wenn eine wirksame, an den jeweiligen Einsatzfall angepaßte Sicherung der Verstelleinrichtung vorhanden ist.	
Unbeabsichtigtes Herausdrehen des Stellteils der Verstelleinrichtung	Ja, wenn eine wirksame formschlüssige Sicherung gegen das Herausdrehen vorhanden ist.	
Bersten des Gehäuses oder Bruch von Deckel-, Befestigungs- oder Verbindungselementen	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Anordnung im System und Befestigung den Regeln der Technik entsprechen.	

Tabelle B.14: Schalldämpfer

Fehlerannahme	Fehlerausschluß	Bemerkungen
Zusetzen (Verstopfen) des Schalldämpferelementes	Ja, wenn Konstruktion und Ausführung des Schalldämpferelementes Bemerkung 1) erfüllen.	1) Das Verstopfen des Schalldämpferelementes und/oder eine Erhöhung des Staudruckes in der Abluft über einen kritischen Wert hinaus ist unwahrscheinlich, wenn der Schalldämpfer einen entsprechend großen Querschnitt hat und so konstruiert ist, daß er die Betriebsbedingungen erfüllt.
Unbeabsichtigtes Herausdrehen des Schalldämpferelementes	Ja, wenn eine wirksame, formschlüssige Sicherung gegen das Herausdrehen vorhanden ist.	
Bruch/Bersten des Schalldämpfergehäuses oder Ausreißen des Befestigungsgewindes	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Anordnung im System und Befestigung den Regeln der Technik entsprechen.	

B.4.5 Energiespeicher und Druckbehälter

Tabelle B.15: Energiespeicher und Druckbehälter

Fehlerannahme	Fehlerausschluß	Bemerkungen
Bruch/Bersten des Energiespeichers/Druckbehälters oder der Verbindungselemente oder Ausreißen der Gewinde von Befestigungsschrauben	Ja, wenn Konstruktion, Auswahl der Einrichtungen, Auswahl der Werkstoffe und Anordnung im System den Regeln der Technik entsprechen (siehe Bemerkung 1)).	1) Es könnten auch die Anforderungen der Richtlinien 87/404/EWG und 90/488/EWG für einfache Druckbehälter und der Richtlinie 97/23/EG für Druckgeräte einschließlich der dort erfaßten zutreffenden Regeln zu beachten sein.

B.4.6 Sensoren

Tabelle B.16: Sensoren

Fehlerannahme	Fehlerausschluß	Bemerkungen
Ausfall des Sensors (siehe Bemerkung 1))	Nein	1) Sensoren in dieser Tabelle schließen die Signalerfassung, -verarbeitung und -ausgabe besonders für Druck, Volumenstrom, Temperatur und Weg ein.
Veränderung der Erfassungs- oder Ausgabecharakteristiken	Nein	

B.4.7 Informationsverarbeitung

Tabelle B.17: Verknüpfungsglieder

Fehlerannahme	Fehlerausschluß	Bemerkungen
Ausfall des Verknüpfungsgliedes (z. B. UND-Glied, ODER-Glied, Speicherglied) durch z. B. Veränderung der Schaltzeiten, Nichtschalten oder unvollständiges Schalten	Für entsprechende Fehlerannahmen und Fehlerausschlüsse siehe Tabellen B.4, B.5 und B.6.	

Tabelle B.18: Verzögerungsglieder

Fehlerannahme	Fehlerausschluß	Bemerkungen
Ausfall des Verzögerungsgliedes (z. B. pneumatische und pneumatisch/mechanische Zeit- und Zählglieder)	Ja, bei Verzögerungsgliedern ohne bewegte Bauteile, z. B. Festwiderstände, wenn übliche Betriebsbedingungen vorliegen (siehe Bemerkung 1)) und die Druckluft ausreichend aufbereitet und filtriert wird.	1) Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen eingehalten wurden.
Veränderung der Erfassungs- oder Ausgabecharakteristiken		
Bersten des Gehäuses oder Bruch der Deckel- oder Befestigungselemente	Ja, wenn Konstruktion, Dimensionierung und Einbau den Regeln der Technik entsprechen.	

Tabelle B.19: Umformer

Fehlerannahme	Fehlerausschluß	Bemerkungen
Fehlerhafter Umformer (siehe Bemerkung 1))	Ja, bei Umformern ohne bewegte Bauteile, z. B. Reflexdüse, wenn übliche Betriebsbedingungen vorliegen (siehe Bemerkung 2)) und die Druckluft ausreichend aufbereitet und filtriert wird.	1) Hier werden z. B. Bauelemente für die Umformung eines pneumatischen Signals in ein elektrisches Signal, die Erfassung von Positionen (Zylinderschalter, Reflexdüse) und die Verstärkung pneumatischer Signale betrachtet. 2) Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen eingehalten wurden.
Veränderung der Erfassungs- und Ausgabecharakteristik		
Bersten des Gehäuses oder Bruch der Deckel- oder Befestigungselemente	Ja, wenn Konstruktion, Dimensionierung und Einbau den Regeln der Technik entsprechen.	

Anhang C (informativ)

Möglichkeiten zur Validierung hydraulischer Systeme

Inhalt

	Seite
C.0 Einleitung	37
C.1 Liste der grundlegenden Sicherheitsprinzipien	38
Tabelle C.1: Grundlegende Sicherheitsprinzipien	38
C.2 Liste der bewährten Sicherheitprinzipien	40
Tabelle C.2: Bewährte Sicherheitsprinzipien	40
C.3 Liste der bewährten Bauteile	41
Tabelle C.3: (leer)	41
C.4 Fehlerlisten und Fehlerausschlüsse	41
C.4.0 Einleitung	41
C.4.1 Ventile	42
Tabelle C.4: Wegeventile	42
Tabelle C.5: Rückschlagventile, Sperrventile (Sitzventile)	44
Tabelle C.6: Stromventile	45
Tabelle C.7: Druckventile	46
C.4.2 Leitungen	47
Tabelle C.8: Rohrleitungen	47
Tabelle C.9: Schlauchleitungen	47
Tabelle C.10: Verbindungselemente	48
C.4.3 Filter	48
Tabelle C.11: Filter	48
C.4.4 Energiespeicher	49
Tabelle C.12: Energiespeicher	49
C.4.5 Sensoren	49
Tabelle C.13: Sensoren	49

C.0 Einleitung

Bei Anwendung hydraulischer Systeme in Verbindung mit anderen Technologien sollten auch die zutreffenden Tabellen für grundlegende und bewährte Sicherheitsprinzipien berücksichtigt werden. Wo Ventile elektrisch angesteuert werden, sollten die entsprechenden Fehlerlisten im Anhang D berücksichtigt werden.

C.1 Liste der grundlegenden Sicherheitsprinzipien

Tabelle C.1: Grundlegende Sicherheitsprinzipien

Grundlegende Sicherheitsprinzipien	Bemerkungen
Anwendung geeigneter Werkstoffe und Herstellungsverfahren	Auswahl des Werkstoffs, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von z. B. Spannungen, Haltbarkeit, Elastizität, Reibung, Verschleiß, Korrosion, Temperatur.
Richtige Dimensionierung und Formgebung	Berücksichtigen z. B. von Spannungen, Dehnungen, Ermüdung, Oberflächenrauheit, Toleranzen, Hängenbleiben, Herstellung.
Geeignete Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau der Bauteile/des Systems	Berücksichtigen von Anwendungshinweisen des Herstellers (z. B. Katalogblätter, Einbauanweisungen, Festlegungen) sowie von Erfahrungen mit ähnlichen Bauteilen/Systemen.
Anwendung des Prinzips der Energietrennung	Der sichere Zustand wird erreicht, indem alle wichtigen Einrichtungen von der Energiequelle abgetrennt werden. Siehe Primärmaßnahmen zum Anhalten in EN 292-2 : 1991, 3.7.1. Zum Starten der Bewegung eines Mechanismus wird Energie benötigt. Siehe Primärmaßnahmen zum Starten in EN 292-2 : 1991, 3.7.1. Unterschiedliche Betriebsarten sind zu berücksichtigen (z. B. Betriebsmodus, Wartungsmodus). In Sonderfällen können Ausnahmen möglich sein (z. B. dann, wenn der Verlust der hydraulischen Energie eine zusätzliche Gefährdung erzeugt).
Geeignete Befestigung	Zur Anwendung z. B. von Schraubensicherungen, Armaturen, Klebungen, Spannringen, beachten der Anwendungshinweise des Herstellers. Die Anwendung des richtigen Drehmoments ist die Voraussetzung für: a) das Festziehen und b) die Nichtüberlastung von Schrauben und Armaturen.
Druckbegrenzung	Beispiele sind Überdruckventile, Druckminder-/Druckregelventile.
Begrenzung/Verringerung der Geschwindigkeit	Ein Beispiel ist die Geschwindigkeitsbegrenzung eines Kolbens durch ein Stromventil oder eine Drossel.
(fortgesetzt)	